

(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION
EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété
Intellectuelle
Bureau international



(43) Date de la publication internationale
7 août 2003 (07.08.2003)

PCT

(10) Numéro de publication internationale
WO 03/065681 A1

(51) Classification internationale des brevets⁷ :

H04L 29/06, 29/08

(74) Mandataire : PONCET, Jean-François; Cabinet Poncet,
7, chemin de Tillier, B.P. 317, F-74008 Annecy Cedex (FR).

(21) Numéro de la demande internationale :

PCT/FR03/00288

(81) États désignés (*national*) : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(22) Date de dépôt international :

31 janvier 2003 (31.01.2003)

(25) Langue de dépôt :

français

(26) Langue de publication :

français

(30) Données relatives à la priorité :

02/01435

1 février 2002 (01.02.2002) FR

(84) États désignés (*régional*) : brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, SE, SI, SK, TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

(71) Déposant (*pour tous les États désignés sauf US*) :
TRUSTED LOGIC [FR/FR]; 5, rue du Bailliage,
F-78000 Versailles (FR).

(72) Inventeur; et

(75) Inventeur/Déposant (*pour US seulement*) : VETIL-
LARD, Eric [FR/FR]; 1, Passage des Pignes, F-06560
Valbonne (FR).

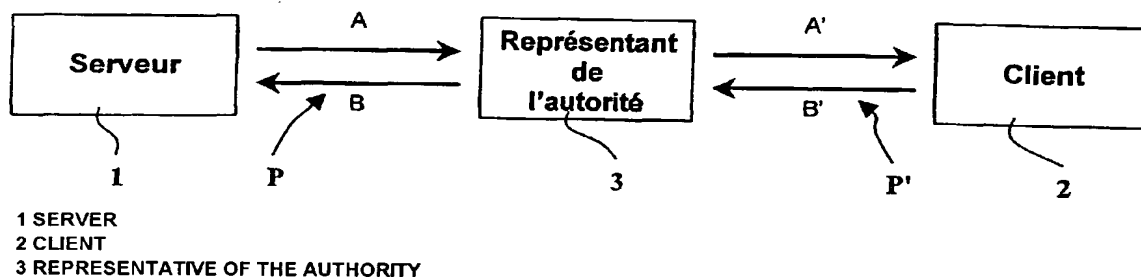
Déclaration en vertu de la règle 4.17 :

— relative à la qualité d'inventeur (règle 4.17.iv)) pour US
seulement

[Suite sur la page suivante]

(54) Title: METHOD AND DEVICE FOR SECURING MESSAGES EXCHANGED IN A NETWORK

(54) Titre : PROCEDE ET DISPOSITIF POUR SECURISER LES MESSAGES ECHANGES SUR UN RESEAU



(57) Abstract: In order to secure messages that are exchanged in a data transmission network between a server (1) and a client (2), a control device that is decentralized or represents the authority (3) is permanently inserted into the network between the server (1) and the user (2) during the secured exchange of messages. Said representative of the authority (3) translates the transmitted messages and carries out the message verifications that have been decided by the authority. Said representative of the authority (3) can be a specific microprocessor card, for example, which is permanently inserted between the server (1) and the client (2), whereby the authority does not need to be directly involved in the transactions and no permanent connection with the authority is required.

(57) Abrégé : Pour sécuriser les messages échangés sur un réseau de transmissions de données entre un serveur (1) et un client (2), on intercale un dispositif de contrôle décentralisé ou représentant de l'autorité (3) en permanence dans le réseau entre le serveur (1) et le client (2) pendant l'échange sécurisé des messages. Le représentant de l'autorité (3) effectue une traduction des messages transmis, et effectue sur les messages transmis les contrôles décidés par l'autorité. Ce représentant de l'autorité (3) peut par exemple être une carte à microprocesseur spécifique, intercalée en permanence entre le serveur (1) et le client (2). L'autorité peut donc ne pas être directement dans les transactions, et il n'est pas besoin d'une connexion permanence avec l'autorité.